Abstract

Curtained operation provides trusted execution of code and secrecy of data in a secure memory. Curtained code can only be executed from within certain address ranges of a curtained memory region secure against access by code from without the region. Code entry points are restricted, and atomic execution is assured. The memory is organized into multiple hierarchically curtained rings, and peer subrings are denied access to each other as well as to more secure rings.